PIER Energy System Integration Program Area

Enterprise Information Security (EIS) - Program 86

Contract #: 500-00-023 **Project #:** 52
Contractor: Electric Power Research Institute (EPRI)
Project Amount: $45,000
Match Amount: $1,421,096
Contractor Project Manager: Jim Fortune (650) 855-2500
Commission Contract Manager: Laurie ten Hope (916) 654-4637
Status: Completed

Project Description:
The purpose of this project is to address concerns over the security of the energy industry's electronic infrastructure against cyber threats. These threats range from corporate espionage by competitive rivals to sabotage by hackers or terrorists. Immediate concerns center on the vulnerabilities of electronic operations systems such as supervisory control and data acquisition (SCADA) and plant distributed control systems (DCS) and their interconnectivity with corporate business systems. As the energy industry becomes increasingly automated and electronically connected, a concerted cyber attack could be catastrophic from business, customer and national security perspectives.

This EPRI program identifies and addresses security issues through a series of meetings and workshops that provide forums for sharing information on best practices, lessons learned, and vulnerability assessment results. In addition, the program focuses on the development, application, and testing of technical solutions.

This project supports the PIER Program objective of:

- Improving the reliability of California's electricity by leveraging the collective knowledge of the participants to develop strategies for protecting the State's critical electric power infrastructure against cyber threats.

Proposed Outcomes:

1. Organize and facilitate workshops for collaborative exchange of information and ideas to support the development of robust security programs.
2. Provide security guidelines covering critical security activities and policies and procedures, all reflecting the collective knowledge of the industry.
3. Provide security enhancements that reduce the vulnerability of control centers, SCADA systems, power plant controls, field devices, customer electronic meters, and the protocols used to communicate with these devices, while meeting operational needs.
4. Enhance the risk assessment framework developed in 2001 to help decision makers understand and evaluate the costs and benefits of different security measures.

Actual Outcomes:

1. Workshops
    - Three topical workshops were delivered in 2002.
2. Guidelines, Policies and Procedures
    - EPRI published a report, *Security Vulnerability Self-Assessment Guidelines for the Electric Power Industry* (1001639), that provides detailed guidelines and technical information that will assist any organization engaged in generating, transmitting, distributing, or marketing electric power in performing its own security self-assessment.
3. Security Enhancements
    - EPRI published a report, *ICCP (TASE.2) Security Enhancements: Executive Summary* (1001641) that summarizes the current security enhancements that EPRI is recommending to secure the ICCP. The detailed recommendations are presented in EPRI report 1001642.
    - A technical report, *ICCP (TASE.2) Security Enhancements: Volume 1* (1001642), was published that details the security requirements for the Inter-Control Center Communications Protocol (ICCP-IEC60870-6 TASE.2), also known as TASE.2. Based on these requirements, the report assesses the current ICCP for potential vulnerabilities and recommends solutions.
    - A technical update report, *Security Enhancements for Utility Information Architectures* (1002651) was published. It presents the results of a study conducted to assess the impact on performance of the security measures being proposed for the common protocols used for digital control of power system equipment, and to determine what additional security measures outside the domain of protocols may be needed for complete end-to-end security.
4. Risk Assessment Framework
    - A web-accessible risk assessment framework was completed in 2002.

Project Status:
The project has been completed.

"Research Powers the Future"